Rewriting Homework
A rendre au plus tard le 8 janvier 2016

In what follows $\mathcal{R}$ is a finite term rewriting system on the function symbols $\mathcal{F}$. $\mathcal{F}$ is assumed to contain infinitely many constant symbols $\{a_i \mid i \in \mathbb{N}\}$, which we do not recall in the examples.[1] We use the symbol $\top$ for an empty set of equations, or the identity substitution.

We recall that an *idempotent substitution* ϕ is a mapping from a finite set of variables $\mathtt{Dom}(\phi)$ (called its *domain*) to $T(\mathcal{F}, X \setminus \mathtt{Dom}(\phi))$. A solution (in the free algebra) of a se $s_1 \stackrel{?}{=}_\emptyset t_1 \wedge \dots s_n \stackrel{?}{=}_\emptyset t_n$ is an idempotent substitution σ such that, for all i, $s_i\sigma = t_i\sigma$. Such a set of equations either has no solution or has an idempotent mgu (most general unifier) μ such that μ is a solution and all other solutions σ can be written $\sigma = \mu\theta$. Deciding whether there is a solution or not and, in case there is one, computing an idempotent mgu, can be completed in linear time.

An mgu $\{x_1 \mapsto u_1; \dots x_k \mapsto u_k\}$ is identified with a solved system $x_1 \stackrel{?}{=}_\emptyset u_1 \wedge \dots \wedge x_k \stackrel{?}{=}_\emptyset u_k$.

The goal here is to extend unification procedures to solve equations in quotients $T(\mathcal{F})/\xleftrightarrow[\mathcal{R}]{*}$ where $\mathcal{R}$ is a confluent term rewriting system.

An *equation system* S is a formula

$$\exists x_1, \dots, x_m.\ u_1 \stackrel{?}{=}_\mathcal{R} v_1 \wedge \dots u_n \stackrel{?}{=}_\mathcal{R} v_n \qquad \| \quad \phi$$

where $u_1, \dots, u_n, v_1, \dots, v_n \in T(\mathcal{F}, X)$, and ϕ is an idempotrent substitution (the solved part of the system), whose domain is disjoint from $\{x_1, \dots, x_n\}$.

All equations are assumed to be symmetric: we make no distinction between $u \stackrel{?}{=}_\mathcal{R} v$ and $v \stackrel{?}{=}_\mathcal{R} u$ (resp. $u \stackrel{?}{=}_\emptyset v$ and $v \stackrel{?}{=}_\emptyset u$).

A *solution* of an equation system $\exists x_1, \dots, x_m.\ u_1 \stackrel{?}{=}_\mathcal{R} v_1 \wedge \dots u_n \stackrel{?}{=}_\mathcal{R} v_n \ \| \ \phi$ is a substitution σ from $\mathtt{Dom}(\sigma) \subseteq \mathtt{Var}(u_1, v_1, \dots, u_n, v_n, \phi) \setminus \{x_1, \dots, x_m\}$ to $T(\mathcal{F})$ such that there is a substitution θ, from $x_1, \dots, x_m$ to $T(\mathcal{F})$, such that

1. for every $i = 1, \dots, n$,
$$u_i\sigma\theta \xleftrightarrow[\mathcal{R}]{*} v_i\sigma\theta$$
2. there is a substitution θ' such that, $\sigma\theta = \phi\theta'$

An equation system is *in solved form* if it is of the form $\exists\vec{x}.\quad \top \quad \| \quad \phi$.

Consider the following transformation rules, in which the variables of the rules in $\mathcal{R}$ are renamed each time it is necessary.

(**Block**) $\exists\vec{x}.\quad u \stackrel{?}{=}_\mathcal{R} v \wedge S \quad \| \quad \phi \quad \rightsquigarrow \quad \exists\vec{x}.\quad S\sigma \quad \| \quad \sigma$
If σ is a m.g.u of $u \stackrel{?}{=}_\emptyset v \wedge \phi$

(**Narrow**) $\exists\vec{x}.\quad u \stackrel{?}{=}_\mathcal{R} v \wedge S \quad \| \quad \phi \quad \rightsquigarrow \quad \exists.\vec{x}, \vec{y}.\quad u[r]_p\sigma \stackrel{?}{=}_\mathcal{R} v\sigma \wedge S\sigma \quad \| \quad \sigma$
if $\vec{y} = \mathtt{Var}(l \to r)$, $l \to r \in \mathcal{R}$,
p is a non-variable position of u,
σ is a mg.u. of $l \stackrel{?}{=}_\emptyset u|_p \wedge \phi$,
$\vec{y} \cap \mathtt{Var}(u, v, S) = \emptyset$

[1] Adding such constant symbols, standing for the variables in $T(\mathcal{F}, X)$ prevents from confusing the syntax of the problems and their interpretation. It is not a restriction on the problems that are considered.

A *derivation* is a sequence of equation systems E_i such that $E_0 \rightsquigarrow \cdots \rightsquigarrow E_i \rightsquigarrow \cdots$ and each derivation step relies on one of the two above rules. The solved forms of an equation system S are all systems S' in solved form that can be obtained by a derivation starting with S.

We will show below that this yields a procedure for solving equation systems for an arbitrary convergent $\mathcal{R}$.

Question 1

Consider the following (ground) rewrite system on $\mathcal{F} = \{f(1), g(1), a(0), b(0)\}$

$$\mathcal{R}_0 = \begin{cases} f(g(a)) & \rightarrow & f(b) \\ g(f(b)) & \rightarrow & g(a) \end{cases}$$

and the equation system $E_0 = f(g(x)) \stackrel{?}{=}_{\mathcal{R}} f(y) \quad \| \quad \top$.

Give all possible derivations starting from E_0 and yielding a solved form.

Question 2

Consider the following rewrite system on $\mathcal{F} = \{\mathsf{enc}(2), \mathsf{dec}(2), \pi_1(1), \pi_2(2), \langle \_, \_ \rangle (2)\}$:

$$\mathcal{R}_1 = \begin{cases} \mathsf{dec}(\mathsf{enc}(x, y), y) & \rightarrow & x \\ \pi_1(\langle x, y \rangle) & \rightarrow & x \\ \pi_2(\langle x, y \rangle) & \rightarrow & y \end{cases}$$

Give all possible derivations starting from $\pi_1(\mathsf{dec}(x, y)) \stackrel{?}{=}_{\mathcal{R}} y \| \top$. (2 possible derivations).

Question 3

Show that, if $S \rightsquigarrow S'$, then the solutions of S' are contained in the solutions of S

Question 4

1. Assume that $\mathcal{R}$ is terminating and confluent. A substitution σ is then *normalized* if, for every variable x, $x\sigma$ is irreducible.

   Show that, if σ is a normalized solution of $E = \exists \vec{x}.\ S \| \phi$, $S\phi = S$ and $S \neq \top$, then there is a E' such that $E \rightsquigarrow E'$ and σ is a solution of E'.

2. Show that any normalized solution of an equation system $S \| \top$ is a solution of one of its soved forms.

   Deduce a procedure for solving equations in the quotient $T(\mathcal{F}) / \xleftrightarrow[\mathcal{R}]{*}$ for convergent rewrite systems $\mathcal{R}$.

3. Give an example showing that this result is incorrect when $\mathcal{R}$ is terminating but not confluent.

4. Give an example of a confluent $\mathcal{R}$, an equation system $E = u \stackrel{?}{=}_{\mathcal{R}} v \| \top$ and a solution σ such that for every E' such that $E \rightsquigarrow E'$ and for every σ' such that, for every variable x, $x\sigma' \xleftrightarrow[\mathcal{R}]{*} x\sigma$, σ' is not a solution of E'. (Hence termination is necessary)

Question 5

Consider the rewrite system

$$\mathcal{R}_2 = \left\{ \begin{array}{rcl} 0 + x & \to & x \\ s(x) + y & \to & s(x + y) \end{array} \right.$$

1. Explain why $\mathcal{R}_2$ is confluent
2. Using the automatic procedure of the previous question, give the solved forms of the equation systems
   (a) $x + y \stackrel{?}{=}_{\mathcal{R}} s(s(0))$.
   (b) $x + 0 \stackrel{?}{=}_{\mathcal{R}} x$

Question 6

We replace here the **Narrow** rule with

$$(\textbf{Narrow}) \quad \exists \vec{x}. \quad u \stackrel{?}{=}_{\mathcal{R}} v \wedge S \quad \| \quad \phi \quad \rightsquigarrow \quad \exists . \vec{x}, \vec{y}. \quad u[r]_p \stackrel{?}{=}_{\mathcal{R}} v \wedge S \quad \| \quad \sigma$$
$$\begin{array}{l} \text{if } \vec{y} = \mathtt{Var}(l \to r),\ l \to r \in \mathcal{R} \\ p \text{ is a non-variable position of } u, \\ \sigma \text{ is a mg.u. of } l \stackrel{?}{=}_{\emptyset} u|_p \wedge \phi, \\ \vec{y} \cap \mathtt{Var}(u, v, S) = \emptyset \end{array}$$

In other words, the unifier σ is not applied to the unsolved part of the equations. (This is known as the *basic strategy*).

1. Show that this restriction is harmless: in case $\mathcal{R}$ is convergent, the results of the questions 3 and 4 still hold true with this strategy.
2. How does it help for the examples of question 5 ?

Question 7

Show that, if $\mathcal{R}$ is confluent and if every right hand side of a rule is a subterm of the corresponding left-hand side, then the procedure derived from question 6 is terminating.

Would it be also the case with the procedure derived from question 4 ?